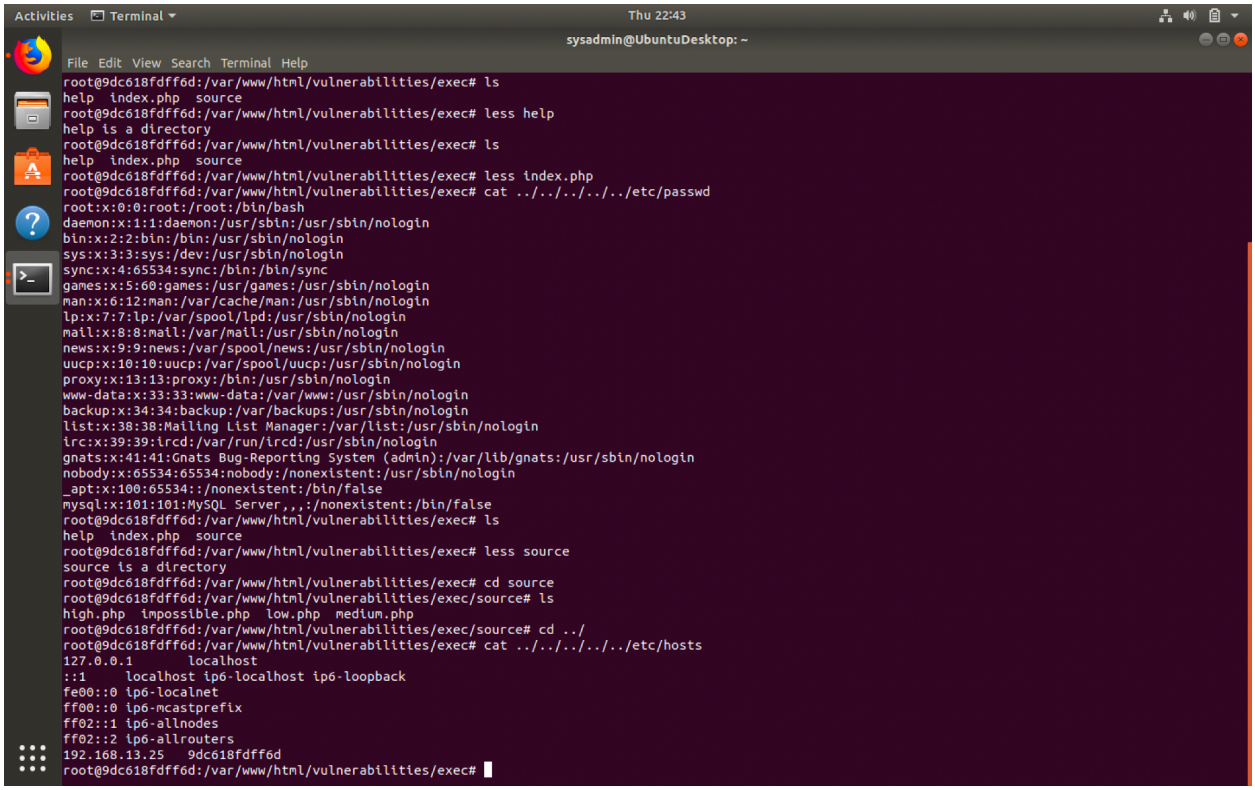
UCSD CyberSecurity Bootcamp

# Web Vulnerabilities and Hardening

**1. Your wish is my command injection:**



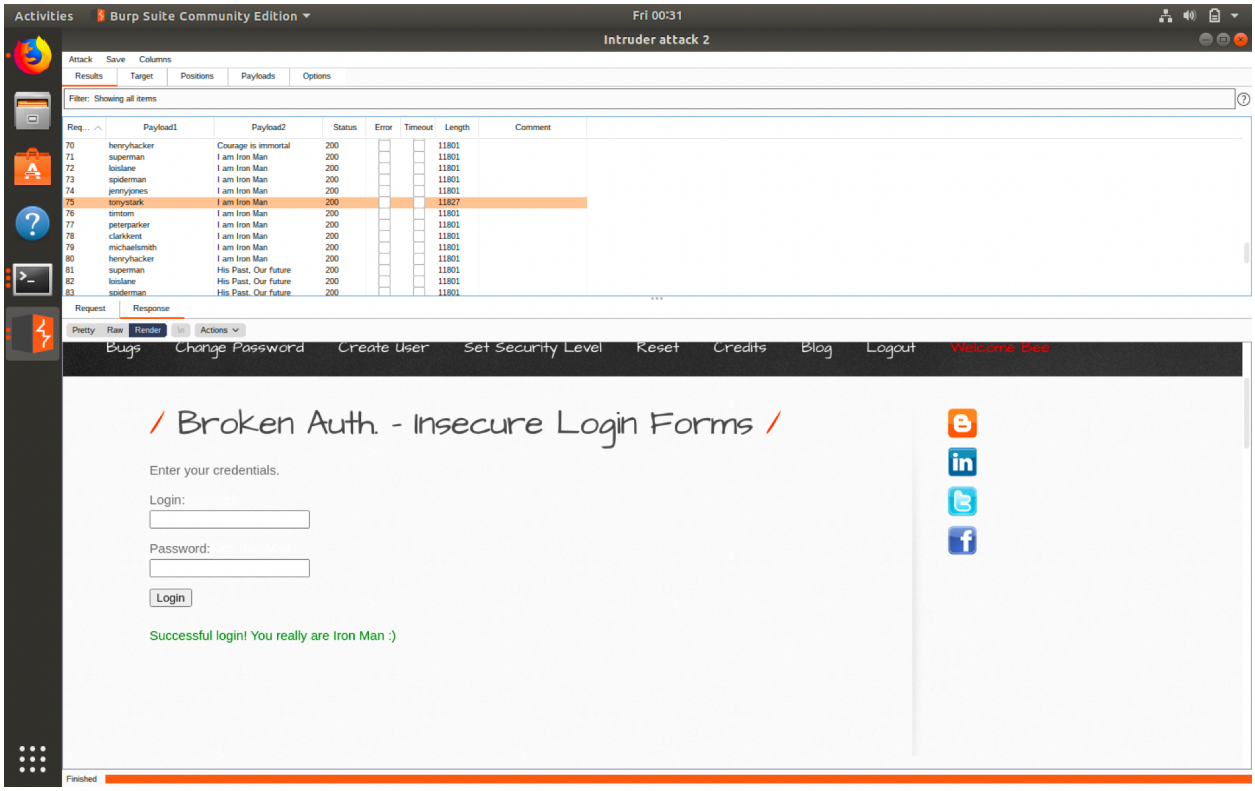

For the mitigation for the above command injection attack, it is recommended that you harden the website.

1. Input validation code- This would ensure that only properly formed data would enter the information system. All data from untrusted sources would be subject to this, thus preventing malware or command injections. You can also use only whitelisted characters.

2. Update the Application as well as patch the system or application.

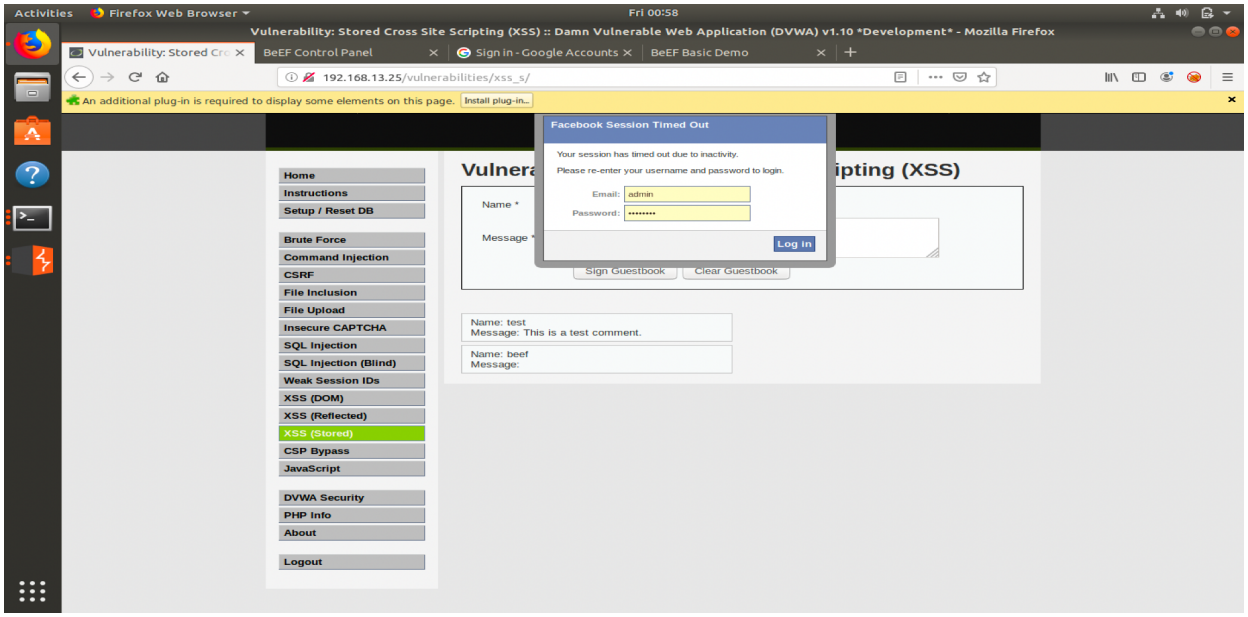
3. You can also use the principle of least privilege to only allow the application or processes the minimum requirements for the task.

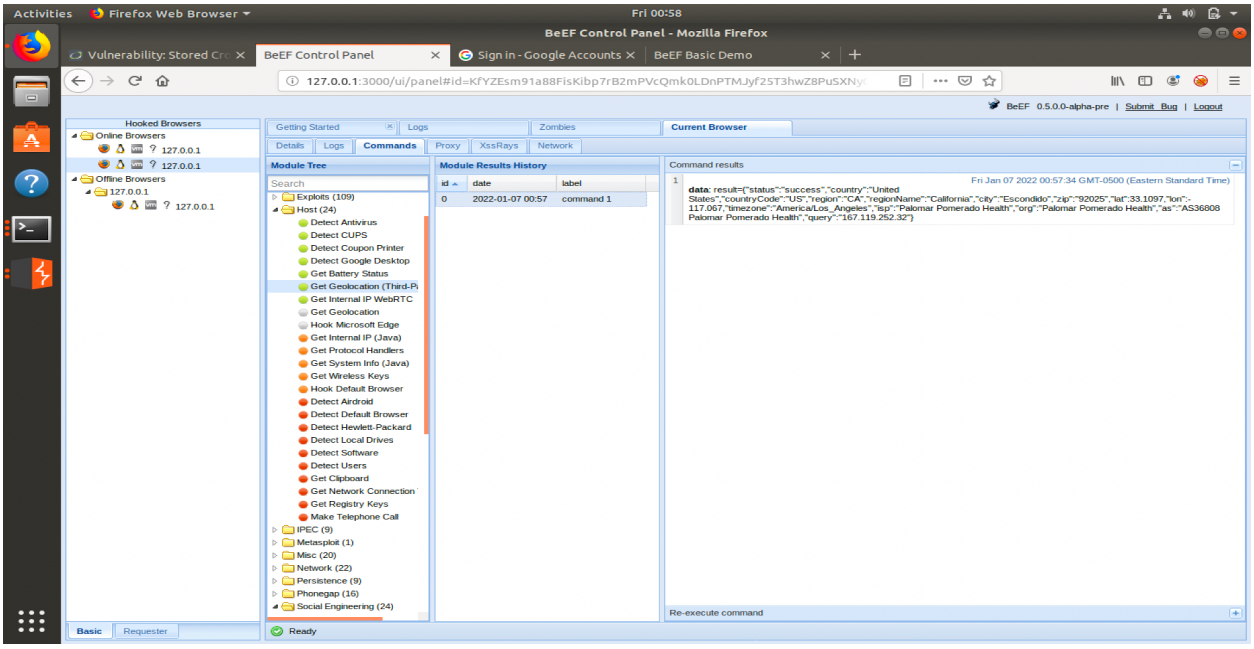
## 2.A Brute Force to Be Reckoned With




Mitigation strategies for a brute force attack such as this are mitigated by locking down the password attempts that can be executed preventing the use of a password cracker. If this is done the attacker will lose the chance to use a password cracker such as John the Ripper. You could also lock out authentication attempts from trusted or untrusted browsers.

## 3. Where's the BeEF?



**Mitigation Strategies:**

In order to prevent web application attacks there are many ways to harden the security to prevent as many attacks as possible. The first is to implement and redirect all HTTP traffic to HTTPS. You can also use a program such as keypass to generate and store much more and secure strong passwords. As well you can implement a web application firewall.